SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Mai 2014

SWITCH

I. Android prüft zukünftig kontinuierlich installierte Apps – Fake-Virenscanner ist Shooting Star in Googles App-Store

Geräte mit Googles Mobile-Betriebssystem Android sollen künftig kontinuierlich nach bösartigen Apps suchen. Und zwar, indem sämtliche installierten Programme durch die Funktion «Verify Apps» regelmässig auf anormales Verhalten untersucht werden («on-device monitoring»). Bislang erfolgt ein solcher Sicherheitsscan nur einmal bei der Installation einer App – und nur dann, wenn sie nicht von Googles eigenem App-Store kommt. Per Update will Google «Verify Apps» allen Nutzern von Android (ab Version 2.3) zur Verfügung stellen.

Auf alle Fälle sollte sich der Konzern mit dem Rollout beeilen: Gerade haben Forscher von «FireEye» herausgefunden, dass sich bösartige Apps auf Android-Geräten heimlich an anderen installierten Apps zu schaffen machen können. Indem sie die Rechteverwaltung anderer Apps auf dem System ausnutzen und so etwa hinterlegte Verknüpfungen manipulieren. Das kann unter anderem dazu führen, dass die Mobile-Banking-App auf dem eigenen Smartphone nicht mehr zur korrekten Bankenanwendung führt, sondern auf eine manipulierte Phishing-Version davon.

Angreifer könnten so an die Kundendaten der Nutzer gelangen, warnen die Forscher. Eine App, die für genau so etwas sorgt, konnten die Forscher zudem problemlos in Googles Play-Store platzieren.

Wer sein Android-Gerät mit zusätzlichen Apps schützen will, sollte sich übrigens vorab genau informieren: Gerade musste Google einen vollkommen wirkungslosen Pseudo-Virenscanner aus dem Geschäft ziehen. Die Securityleute der «Android Police» hatten das Programm in Googles Play-Store als «Fake Security App» entlarvt: «Das einzige, was die App tut, ist, das Bild eines ‚X' nach einmaligem Antippen in ein ‚check'-Bild zu verwandeln.»

Dass es ausgerechnet ein solches offensichtlich betrügerisches Programm auf Platz eins der Bezahl-Apps in Googles Play-Store geschafft hat, empfinden die Experten der «Android Police» als «entmutigend». Im Interview mit dem britischen «Guardian» bezeichnete der Entwickler das Ganze als «törichten Fehler» ohne böse Absicht. Allerdings ist diese wirkungslose App kein Einzelfall. Google will die Tausende von betrogenen Nutzern jetzt entschädigen.

Nachzulesen unter:

http://officialandroid.blogspot.ch/2014/04/expanding-googles-security-services-for.html
http://www.fireeye.com/blog/technical/2014/04/occupy_your_icons_silently_on_android.html
http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/

II. US-Behörde schafft vollendete Tatsachen in Sachen Netzneutralität

Wer es sich leisten kann, kann künftig seine Datenpakete schneller im Netz verbreiten als die Konkurrenz. Die Grundlagen dafür hat soeben die US-Aufsichtsbehörde «Federal Communications Commission» (FCC) geschaffen.
Demnach soll es in den USA so etwas wie eine Überholspur für Datenpakete auf der letzten Meile zum Kunden geben. Damit ist die so genannte Netzneutralität – eine der Grundfesten der Väter des Internets – de facto gekippt. Bislang galt im Internet das Prinzip, dass alle Informationen gleichberechtigt weitergeleitet werden, niemand hatte «Vorfahrt».

Laut FCC-Vorsitzendem Tom Wheeler könnten Netzneutralität und «Web Fast Lane» friedlich koexistieren. So sollen Provider zwar Geld verlangen dürfen, aber keine Exklusiv-Deals abschliessen können. Konkurrenten muss ein «wirtschaftlich vernünftiges» Angebot gemacht werden, ebenfalls eine Überholspur zu mieten. Für Start-ups würden sich dennoch unüberwindbare Hürden auftun, schreibt das IT-Newsportal «Futurezone».

Für Internet-Pioniere, Netzaktivisten und viele, die massgeblich am Aufbau des World Wide Web beteiligt waren, ist damit der Weg bereitet für die Zwei-Klassen-Gesellschaft im Internet. Klare Worte findet auch Craig Aaron, CEO von «Freepress.net»: «Mit diesem Vorschlag hilft die FCC den grössten ISPs in deren Bemühungen, das offene Internet zu zerstören.» Michael Weinberg, Vice President von «Public Knowledge» äussert sich so: «Die FCC lädt ISPs dazu ein, Gewinner und Verlierer im Internet zu bestimmen. Die Essenz eines ‚wirtschaftlich angemessenen' Standards ist Diskriminierung. [...] Das ist nicht Netzneutralität.»

Am 15. Mai will die FCC die neuen Regeln formell verabschieden. Noch sind Änderungen möglich. Und sie würden auch nur für die Vereinigten Staaten gelten. Eine Signalwirkung für Europa ist allerdings nicht auszuschliessen.

Weiterführende Infos:

http://futurezone.at/netzpolitik/offenes-internet-in-den-usa-vor-dem-ende/62.192.252
https://netzpolitik.org/2014/netzneutralitaet-in-den-usa-fcc-erlaubt-wirtschaftlich-angemessenene-zerstoerung-des-internets/
http://www.freepress.net/press-release/106177/fcc-proposal-payola-internet-would-end-net-neutrality
http://www.publicknowledge.org/news-blog/press-release/public-knowledge-statement-on-updated-net-neutrality-rules
http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/netzneutralitaet-was-die-plaene-der-amerikanischen-fcc-bedeuten-12908307.html

III. «Heartbleed» setzt Frust und Hoffnung der Open-Source-Entwickler frei

Das hat gesessen: Die Sicherheitslücke «Heartbleed» war anscheinend genau das, was es brauchte, um auf die schwierige Situation wichtiger Open-Source-Software, wie «OpenSSL», aufmerksam zu machen. Denn seit Jahren setzen Firmen, Regierungen

und Bürger frei verfügbare Open-Source-Programme ein, ohne sich darum zu scheren, dass deren Weiterentwicklung etwas kostet.

Wegen eines Programmierfehlers in der Krypto-Bibliothek OpenSSL, die im Internet allgegenwärtig ist, konnten Angreifer theoretisch zwei Jahre lang geheime Schlüssel, Passwörter und andere Daten betroffener Systeme auslesen. «Heartbleed ist ein seltener Bug», beschreibt Kryptografie-Experte Matt Blaze die Besonderheit des Fehlers. «Er führt dazu, dass eine Krypto-Bibliothek mehr Daten preisgibt, als sie schützen soll. Damit ist sie schlechter als gar keine Kryptografie.»
Der Fehler war einem ehrenamtlichen OpenSSL-Entwickler unterlaufen und blieb immerhin zwei Jahre lang unentdeckt.

Mittlerweile ist der Bug korrigiert und potenziell bedrohte Internetdienste – auch viele namhafte – haben das Update eingespielt und Sicherheitsvorkehrungen getroffen. Ein unangenehmer Nachgeschmack bleibt jedoch: Die Computerindustrie verlasse sich zunehmend auf offene Quellcodes, die Verantwortung für die Entwicklung und Finanzierung will aber kaum einer übernehmen, kritisiert die neu formierte «Core Infrastructure Initiative» (CII) in einer Pressemitteilung. Eine von der «Linux Foundation» als Reaktion auf Heartbleed gegründete Initiative, die das Ziel hat, wichtige Open-Source-Projekte wie OpenSSL finanziell zu unterstützen.

Auch Steve Marquess, Schatzmeister der «OpenSSL Software Foundation», kritisiert diese Doppelmoral: Seinem Projekt mangele es massiv an Geld, Zeit und Personal, um ein so komplexes und kritisches Softwareprodukt pflegen zu können. Gleichzeitig betrachteten es Firmen und Regierungen weltweit als selbstverständlich, OpenSSL gratis einzusetzen. Angesichts dieses frustrierenden Dauerzustandes sei es «kein Wunder, dass ein paar überlastete Freiwillige den Bug übersehen haben; ein Wunder ist es vielmehr, warum so etwas bisher nicht schon viel öfter passiert ist».

Immerhin ist mit «Heartbleed» etwas Bewegung in die Sache gekommen: Cisco, Dell, Facebook, NetApp, IBM, Google und viele andere Konzerne haben sich nun verpflichtet, die nächsten drei Jahre lang mindestens je 100 000 US-Dollar an die Core Infrastructure Initiative zu spenden.

Mehr zum Thema:

http://www.golem.de/news/openssl-wichtige-fragen-und-antworten-zu-heartbleed-1404-105740.html
http://www.zeit.de/digital/internet/2014-04/openssl-heartbleed-core-infrastructure-initiative
http://veridicalsystems.com/blog/of-money-responsibility-and-pride/
http://www.linuxfoundation.org/news-media/announcements/2014/04/amazon-web-services-cisco-dell-facebook-fujitsu-google-ibm-intel

IV. Dropbox will mit Hilfe von Condoleezza Rice weltweit expandieren

#DropDropbox lautet der Twitter-Hashtag, unter dem sich seit Anfang April grosser Protest gegen den Clouddienst «Dropbox» formiert. Viele der erbosten Nutzer – Private wie Kommerzielle – drohen mit Kündigung, rufen zum Boykott auf oder üben lautstark Kritik. Grund dafür ist die Ankündigung von Dropbox-Chef Drew Houston, Dr. Condoleezza Rice werde künftig im Aufsichtsrat des Dienstes sitzen.
Als ehemalige Aussenministerin und nationale Sicherheitsberaterin von George W. Bush war Frau Rice unter anderem für den Ausbau staatlicher Überwachung verantwortlich, der die NSA-Spionage erst möglich gemacht hatte. Zusammen mit zwei anderen Ex-Regierungsmitgliedern betreibt Rice heute eine Beraterfirma.

In einer Zeit, in der sich Nutzer und Firmen weltweit um die engen Verbindungen von US-Technologiefirmen zur Regierung sorgen, ist Rice' Rekrutierung nach Meinung von Branchenkennern kein geschickter Schritt. IT-Medien weltweit werten die Rekrutierung von Rice in den Dropbox-Aufsichtsrat als grossen PR-Fauxpas und Gefahr für den Schutz der Nutzerdaten.
«Dr. Rice versteht unsere Haltung zu diesen Fragen und unterstützt unsere Verpflichtungen gegenüber unseren Nutzern voll», versuchte Houston aufgeregte Kritiker im Firmenblog zu beschwichtigen. Um die Belange in Sachen Datenschutz und Datensicherheit voranzubringen, bräuchte Dropbox genau jemanden wie die Ex-Aussenministerin.
Ob dies mit diesem polarisierenden «Aushängeschild» gelingen kann, bleibt abzuwarten.

Näheres dazu unter:

https://blog.dropbox.com/2014/04/our-commitment-to-your-rights-and-privacy/
http://www.drop-dropbox.com/
https://news.ycombinator.com/item?id=7566069
http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/datenspeicherdienst-dropbox-nutzer-empoert-ueber-berufung-von-condoleezza-rice-12891125.html

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Der Bundesrat hatte im Juni 2012 die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken verabschiedet. Die Strategie enthält 16 Massnahmen, die in sieben Handlungsfelder eingeteilt sind und bis 2017 umgesetzt werden sollen. Nun liegt ein 30-seitiger Jahresbericht vor, der den Status der vorgesehenen Massnahmen beschreibt.

http://www.news.admin.ch/NSBSubscriber/message/attachments/34670.pdf

Wie lange bleibt ein Useraccount in einem Microsoft Active-Directory noch gültig, nachdem er abgeschaltet oder deaktiviert wurde? Bis zu 10 Stunden, sagen Experten von "Aorato", die das Kerberos Authentifizierungs-Protokoll genauer untersuchten.

http://www.aorato.com/blog/windows-authentication-flaw-allows-deleteddisabled-accounts-access-corporate-data/

Dieser SWITCHcert Security Report wurde von Katja Locker und Frank Herberg verfasst.